UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff*, v. DMITRY STAROVIKOV; ALEXANDER FILIPPOV; and Does 1-15, *Defendants*.	Civil Action No. **FILED UNDER SEAL**

GOOGLE'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION
FOR A TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

This is an application for an emergency ex parte temporary restraining order and an asset restraining order to stop a far-reaching criminal enterprise that has infected over one million computers and other devices with malware and exploits those devices to commit cybercrimes. Each day, thousands of users unknowingly download malware, known as Glupteba, and become part of a botnet of infected computers. And each day, the enterprise targets new victims, infects their devices, obtains access to their accounts, and sells that access to other criminals. This enterprise is the modern, technological incarnation of organized crime. This Court should grant Google's motion to disrupt its operations.

The individuals at the heart of this enterprise threaten harm to Google, its users, and the internet writ large. Although Defendants reside in Russia, they target victims in the United States and New York. Their malware allows them to steal victims' account credentials and to piggyback on a computer's unique IP address, which other criminals purchase to commit a range of crimes and conceal their true identities and locations. Defendants also use the botnet to commit other criminal acts, including facilitating credit card fraud. Without intervention, Defendants' criminal enterprise will continue to enable a range of malicious cyber threats, including ransomware and distributed denial-of-service attacks.

This Court should grant Google's proposed temporary restraining order and order to show cause for a preliminary injunction. The linchpin of Google's requested relief is a disruption plan to disable the domains, IP addresses, and servers used by Defendants to carry out their enterprise and suspend Defendants' control of the botnet. These steps will terminate Defendants' ability to sell access to victims' accounts and computers, as well as disrupt any further criminal activities by disabling Defendants' communication with infected computers.

Google's application establishes the factors necessary to obtain a temporary restraining order and preliminary injunction: irreparable harm, a likelihood of success (or substantial questions) on the merits, a balance of equities tipping in its favor, and relief in the public interest. *Citigroup Glob. Mkts., Inc. v. VCG Special Opportunities Master Fund Ltd.*, 598 F.3d 30, 34 (2d Cir. 2010). *First*, Google and other victims are likely to suffer irreparable harm in the absence of relief. Defendants trick users into downloading malware, then steal and sell access to Google accounts. Thousands of new computers are infected each day and become unknowing soldiers in service of Defendants' criminal enterprise. *Second*, Google is likely to succeed on the merits of its claims (which indisputably raise a "substantial question"). Defendants operate a vast criminal enterprise that has infiltrated over a million devices through deception, including misrepresenting Google's YouTube mark. After infecting devices, Defendants have sold access to Google accounts and then deceived Google into believing that its systems were accessed by the true users of the accounts. This conduct violates the Computer Fraud and Abuse Act, wire fraud, access device, and identity fraud statutes—all predicate acts under the Racketeer Influenced and Corrupt Organizations Act ("RICO")—as well as violations of the Lanham Act and other federal and state laws. *See* 18 U.S.C. §§ 1962(c)–(d), 1030, 2510, 2701. *Finally*, given Defendants' ongoing criminal activity, the balance of equities and public interest also favor injunctive relief.

This Court should also exercise its broad equitable authority under the Lanham Act and Federal Rule of Civil Procedure 64 to freeze Defendants' assets in furtherance of Google's request for an accounting of profits. *See Gucci Am., Inc. v. Weixing Li*, 768 F.3d 122, 131-32 (2d Cir. 2014); *Ayyash v. Bank Al-Madina*, 233 F.R.D. 325, 327 (S.D.N.Y. 2005).

To meaningfully disrupt the botnet, relief must be ex parte. Notice would only give Defendants the opportunity to relocate the infrastructure they use to control the botnet. If this

Court grants preliminary relief, Google will provide Defendants with notice five days before a hearing on a preliminary injunction, through service as requested in this motion.

BACKGROUND

Defendants Dmitry Starovikov and Alexander Filippov, and Does 1 through 15, are Russian cybercriminals who run a modern-day organized crime syndicate with their co-conspirators (collectively, the "Glupteba Enterprise" or "Enterprise"). Compl. ¶¶ 3, 15–18; Declaration of Shane Huntley ("Huntley Decl.") ¶¶ 43, 86–89. The Enterprise deploys Glupteba malware onto computers and other devices around the world. Once infected, these devices become part of the Glupteba botnet—a metastasizing network that the Glupteba Enterprise uses to carry out its illicit schemes without detection by the device user. Compl. ¶¶ 27–31; Huntley Decl. ¶¶ 25, 43, 75–77. The botnet undermines Google's extensive security measures and threatens harm to its relationship with its billions of users. Compl. ¶¶ 29–40, 100–03; Huntley Decl. ¶¶ 28, 49, 51, 65–66. The threat to Google, its users, and the public is significant and growing. The Enterprise has captured more than a million computers and devices worldwide, including in the United States and New York, and adds infected devices to the botnet each day.

A. The Glupteba Botnet

A botnet is a network of devices infected by viruses or other malware and controlled by criminals who often, as in this case, direct its operations from afar. Botnets provide strength in numbers: cybercriminals can use them to marshal the power of many thousands of different devices for a common purpose.

Cybersecurity experts first noticed Glupteba malware in 2011, when it was primarily associated with a spam campaign. But the malware began to spread more broadly starting in 2020. Compl. ¶ 30; Huntley Decl. ¶ 21. The malware infects devices through numerous third-party sites that disguise the malware as free software, videos, or movies available for download. For instance,

at the website video-youtube-get.ru, individuals were deceived into believing they were clicking on a link to download a YouTube video. Compl. ¶ 33; Huntley Decl. ¶ 23. Once they clicked on the link, the Glupteba malware was installed on their devices instead.

Once installed, the Glupteba malware evades detection by hiding the malware from the device's security logs and deactivating antivirus software and other cybersecurity programs. Compl. ¶ 38; Huntley Decl. ¶¶ 24–25. Glupteba is a modular malware, meaning that once it is installed on a device, it can install new modules with different functionality over time as instructed by the bot controller—in this case, the Glupteba Enterprise. Compl. ¶ 35; Huntley Decl. ¶¶ 28–32. The Glupteba malware connects to content delivery network servers to deliver modules to infected devices, the delivery of which is controlled by the Enterprise via command and control ("C2") servers. Compl. ¶¶ 26, 36–41, 48–50; Huntley Decl. ¶¶ 27–42. Through these servers, the Enterprise uses the botnet to carry out myriad illicit schemes. And the malware exploits the infected device's network to infect other devices and grow the botnet.

The Glupteba botnet is particularly pernicious because it is not easy to disable or disrupt. A conventional botnet encodes domain addresses to act as the C2 servers that instruct the infected devices. Compl. ¶ 47; Huntley Decl. ¶ 34; Declaration of Elizabeth A. Bisbee ("Bisbee Decl.") ¶ 17. Disabling those domains can significantly disrupt the botnet. Compl. ¶ 47; Huntley Decl. ¶ 34. But unlike conventional botnets, the Glupteba botnet's C2 servers are not stagnant domain addresses. Compl. ¶ 48; Huntley Decl. ¶ 34. Instead, Glupteba uses blockchain technology—a decentralized database system used to record transactions of cryptocurrency such as Bitcoin—to protect the lines of communication between its C2 servers and the botnet. Compl. ¶¶ 48–50; Huntley Decl. ¶¶ 33–42; Bisbee Decl. ¶¶ 15–20. Blockchain technology is used to store the entire transaction history for a given cryptocurrency on all devices on the cryptocurrency's network.

This protects the information from elimination if a particular device is damaged or otherwise rendered inoperable. Instead of being coded to visit specific domains to retrieve C2 instructions, Glupteba is coded to "search" the Bitcoin blockchain for information in certain Bitcoin addresses that identify the botnet's C2 servers. Compl. ¶¶ 47–50; Huntley Decl. ¶ 37; Bisbee Decl. ¶¶ 21–28. The Glupteba Enterprise periodically makes small transactions with these addresses to provide the locations of "back-up" C2 servers in an encrypted code. Compl. ¶¶ 47–48; Huntley Decl. ¶ 40. If a botnet C2 server goes offline, the malware is programmed to search these transactions in the blockchain for the "new" C2 server. Compl. ¶¶ 48–50; Huntley Decl. ¶¶ 38–42. The botnet's connection to the C2 server is virtually uninterrupted.

B. The Glupteba Enterprise's Criminal Schemes

The Glupteba Enterprise uses the botnet to carry out multiple criminal schemes, including (1) selling virtual access to stolen credentials and cookies from Google and other accounts on the infected devices, (2) selling credit cards for users to fraudulently buy ads on Google and similar ad accounts (including stolen accounts) without paying for those ads, (3) selling the placement of disruptive ads on Glupteba-infected mobile devices, and (4) selling proxy connections to infected devices. *See* Compl. ¶¶ 51–88. These schemes have harmed and will continue to harm users of the Glupteba-infected devices, Google, and others.

Stolen Accounts Scheme. The Enterprise uses Glupteba to harvest data that is maintained on infected computers in internet browsers, including Google Chrome and Google Ads. Compl. ¶ 53; Huntley Decl. ¶ 93. The stolen data includes confidential information such as login credentials (usernames and passwords), URL history, and authentication permissions (cookies). Compl. ¶¶ 53–56; Huntley Decl. ¶¶ 31, 45, 94. Through a website called "Dont.farm," the Glupteba Enterprise in turn sells access to those accounts by loading stolen credentials and cookies of the accounts onto virtual machines. Compl. ¶ 56; Huntley Decl. ¶¶ 45–46. In other words, the

Enterprise's customers pay for the ability to access a browser remotely that is already logged into the victim's Google account. Once granted access to the account, the customer has free rein to use that account however they desire, such as for buying advertisements.

Credit Card Fraud Scheme. Through the Dont.farm website, the Enterprise offers "packages" that include not just access to stolen accounts, but also to credit cards from a website called "Extracard.net" to purchase ads. Compl. ¶¶ 66–69; Huntley Decl. ¶ 56. Customers pay the Enterprise for use of the credit cards on Google Ads or similar accounts but do not pay the bills generated by use of those cards. Compl. ¶ 66; Huntley Decl. ¶¶ 56–60. When a customer of Extracard.net uses the card numbers for purchases, they trick the seller (Google and others) into believing the card is fully funded. Compl. ¶ 67; Huntley Decl. ¶¶ 56–60. Since Google often gives its customers a certain amount of credit to use for purchasing ads before they are charged, Google loses that credited amount when it attempts to recover it from the Extracard.net credit card. Compl. ¶ 67; Huntley Decl. ¶¶ 56–60.

Disruptive Ads Scheme. The Glupteba Enterprise also sells the placement of disruptive ads on Glupteba-infected mobile devices through its website Trafspin.com. Compl. ¶ 72–73; Huntley Decl. ¶ 62. Trafspin.com recently went offline but has apparently been replaced by another website called "Push.farm," which continues to sell disruptive ads pushed to infected mobile devices. Compl. ¶¶ 73–74; Huntley Decl. ¶ 64.

Proxy Scheme. Through its websites, including "AWMProxy.net"[1] and "Abm.net," the Enterprise rents out IP addresses that belong to physical devices infected by Glupteba malware. Compl. ¶¶ 77–83; Huntley Decl. ¶¶ 65–73. The Enterprise's customers pay for the ability to use

[1] On November 23, 2021, AWMProxy.net was rebranded as Vd.net. A blog post on the same day claimed new ownership. *See The Project Has a New Domain and New Owners!*, VD.net (Nov. 23, 2021), https://vd.net/news/the-project-has-a-new-domain-and-new-owners.html.

the infected computers' IP addresses to proxy (or relay) their internet activity through those devices so that they appear to be using an IP address assigned to the infected device. Compl. ¶¶ 77–83; Huntley Decl. ¶¶ 65–73. Cybercriminals who rent these IP addresses can use them to hide their tracks by concealing their true locations and IP addresses. Compl. ¶¶ 77–79; Huntley Decl. ¶¶ 52, 64–73. As a result, security systems that screen for suspicious IP addresses are less likely to detect criminal activity. Compl. ¶ 82; Huntley Decl. ¶¶ 65–73.

C. The Glupteba Criminal Enterprise

The primary individuals behind the Glupteba Enterprise are Defendants Dmitry Starovikov and Alexander Filippov, and Does 1 through 15. Compl. ¶¶ 3, 16–18, 92–95; Huntley Decl. ¶¶ 86–89. *Dmitry Starovikov* is an administrator of Voltonwork.com. Compl. ¶ 94; Huntley Decl. ¶ 88. The secondary email address for the Google Workspace Voltronwork.com account is an email containing Dmitry's name under the Trafspin domain. Compl. ¶ 94; Huntley Decl. ¶ 88. *Alexander Filippov* has email accounts associated with the Google Workspace accounts related to Voltronwork.com, Dont.farm, and Undefined.team. Compl. ¶ 95; Huntley Decl. ¶ 89. Starovikov and Filippov both executed "Terms of Service" for Gmail accounts from the same IP address as one of the botnet's C2 servers used for deploying proxies on infected devices, which establishes their access to a primary driver of the botnet's criminal activities. Compl. ¶¶ 93–95; Huntley Decl. ¶¶ 87–89. Along with their co-conspirators, Defendants direct the Enterprise's criminal schemes through the websites and shell companies they control.

ARGUMENT

This Court should enter Google's proposed temporary restraining order, asset restraining order, and order to show cause for a preliminary injunction to disrupt the Glupteba Enterprise. In addition, this Court should use its power under the All Writs Act to order the reasonable cooperation of third parties, to protect its ability to adjudicate this dispute and award relief.

I. This Court Should Grant Google's Proposed Temporary Restraining Order and Order to Show Cause for a Preliminary Injunction.

A plaintiff is entitled to a temporary restraining order and preliminary injunction where (1) it "is likely to suffer irreparable harm in the absence of" relief, (2) it is "likely to succeed on the merits" (or at least raises "sufficiently serious questions,") (3) the balance of equities tips in [its] favor," and (4) "an injunction is in the public interest." *Citigroup*, 598 F.3d at 34; *see also AIM Int'l Trading, LLC v. Valcucine, SpA*, 188 F. Supp. 2d 384, 386 (S.D.N.Y. 2002) (same).

Courts balance the factors to grant preliminary relief "like a sliding scale," such that "more of one excuses less of the other." *Strougo v. Barclays PLC*, 194 F. Supp. 3d 230, 233 (S.D.N.Y. 2016). Without immediate action to disrupt the botnet, the Glupteba Enterprise will simply continue its criminal activities. All the injunction factors weigh in Google's favor, but given the grave threat of irreparable harm, this Court may grant Google relief if it concludes that Google's claims raise "serious questions going to the merits to make them a fair ground for trial." *Citigroup*, 598 F.3d at 33. Google has met and surpassed this standard.[2]

A. Google and the Public Will Suffer Irreparable Harm Absent Relief.

The Glupteba Enterprise has already infected one million devices with malware. Each day, it infects thousands of new devices, conscripting those machines into tools for its cybercrimes. Compl. ¶ 29; Huntley Decl. ¶¶ 4, 90. That harm is unlikely to ever be compensated—even after final judgment—because the Glupteba Enterprise is controlled by elusive cybercriminals who will take steps to avoid complying with any judgment. "[C]ircumstances[] such as insolvency or

[2] The Second Circuit suggested in *Donziger* that while a private plaintiff may seek permanent injunctive relief under RICO, "interim relief . . . is available only to the United States." *Chevron Corp. v. Donziger*, 833 F. 3d 74, 138 (2d Cir. 2016). Even if this were considered part of the court's opinion and not *dicta*, this Court has authority to grant the interim equitable relief Google seeks under the court's inherent equitable powers, as well as the CFAA, ECPA, and Lanham Act. None of the interim relief Google seeks is authorized only by RICO.

unsatisfiability of a money judgment, can show irreparable harm." *Khepera-Bey v. Santander Consumer USA, Inc.*, 2013 WL 3199746, at *4 (D. Md. June 21, 2013). Google has employed technical measures to protect itself from the harm to its systems caused by this malware, but those actions come at a cost. It has already spent more than 2,000 hours, and well in excess of $100,000, investigating the Glupteba botnet and seeking to protect Google and its users from its misconduct. Huntley Decl. ¶ 95. These expenditures are real, tangible injuries to Google's business.

In addition, Defendants' conduct is tarnishing Google's valuable trademarks, injuring Google's goodwill, and damaging its reputation by creating confusion as to the source of the Glupteba malware and false messages. Consumer confusion and injury to business goodwill constitute irreparable harm. *E.g.*, *Church of Scientology Int'l v. Elmira Mission of Church of Scientology*, 794 F.2d 38, 44 (2d Cir. 1986) (loss to "reputational value and goodwill" are irreparable harm); *Microsoft Corp. v. Does 1–8*, 2015 WL 4937441, at *10 (E.D. Va. Aug. 17, 2015) ("[T]he surreptitious nature of the Shylock botnet is damaging to the Plaintiffs' brands and the customer goodwill engendered by their products and trademarks."). Moreover, Google is entitled to a presumption of irreparable harm upon a showing, as Google makes here, of likelihood of success on its claims under the Lanham Act. 15 U.S.C. § 1116(a).

B. Google Will Succeed on the Merits.

To obtain the relief sought, Google need only show that it is "likely to succeed" or that there are sufficiently "serious question[s] going to the merits to make them a fair ground for trial." *Citigroup*, 598 F.3d at 34. Google not only raises serious questions going to the merits, but it is very likely to succeed on each claim. Google has supported its motion with declarations from experienced investigators detailing the substantial evidence of Defendants' misconduct. Given the strength of this evidence, the likelihood of success weighs heavily in favor of granting relief.

Computer Fraud and Abuse Act (the "CFAA"). Congress enacted the CFAA to combat computer-related crimes and abuses, with a focus on "hacking or trespassing into computer systems or data." *United States v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015). Defendants' conduct violates the CFAA's broad prohibition in at least two ways. *First*, they have (l) intentionally accessed (2) without authorization (3) and thereby obtained information (4) from a "protected computer." *Chefs Diet Acquisition Corp. v. Lean Chefs, LLC*, 2016 WL 5416498, at *6 (S.D.N.Y. Sept. 28, 2016) (quoting 18 U.S.C. § 1030(a)(2)(C)). A "protected computer" is any computer "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). *Second*, Defendants violated the CFAA because they intentionally accessed a protected computer without authorization, causing "damage." *Id.* § 1030(a)(5)(C). "Damage" means "any impairment to the integrity or availability of data, a program, a system, or information." *Id.* § 1030(e)(8); *see United States v. Yücel*, 97 F. Supp. 3d 413, 420 (S.D.N.Y. 2015) (holding that malware designed to extract confidential information from a computer, including login credentials, inflicts "damage").

For a private lawsuit like this one, this misconduct must also have resulted in a "loss" adding up to at least $5,000, or damage affecting 10 or more protected computers, during any one-year period. *See* 18 U.S.C. § 1030(g) (cross-referencing the factors listed in § 1030(c)(4)(A)(i)). The term "loss" includes "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense." *Id.* § 1030(e)(11); s*ee, e.g.*, *Saunders Ventures, Inc. v. Salem*, 797 F. App'x 568, 572–73 (2d Cir. 2019) (considering costs incurred as part of an investigation); *see also Paul Rudolph Found. v. Paul Rudolph Heritage Found.*, 2021 WL

4482608, at *15 (S.D.N.Y. Sept. 30, 2021) (same). Even "lost good will or business could provide the loss figure required." *Id.* (cleaned up).

Google has made this showing. Google's evidence reveals that Defendants infected more than one million computers with malware, including thousands in this judicial district alone, to steal user credentials and access user accounts without permission. Huntley Decl. ¶¶ 4, 92. *First,* because those computers were accessed via the internet, they were "used in interstate or foreign commerce or communication" and thus qualify as "protected computers." *See Valle*, 807 F.3d at 528 (noting that the definition of "protected computer" encompasses, in effect, "all computers with [i]nternet access"). *Second*, the access obtained by the Glupteba Enterprise was "without authorization"; Google's users did not consent to having the Enterprise infiltrate their accounts or sell access to their accounts to others. *Third*, the Enterprise infected these computers with malware to "obtain information," including Google account credentials and URL history, or to "impair the integrity" of that information or those computer systems, including by hijacking their processing power to mine cryptocurrency. Compl. ¶¶ 52–63, 84–87; *see also* Huntley Decl. ¶¶ 75–76; Bisbee Decl. ¶ 40. *Finally*, the damage affected well over 10 computers within a one-year span, and resulted in losses exceeding $5,000 within that timeframe, including the costs Google incurred in responding to the botnet's harmful proliferation (well in excess of $100,000). Huntley Decl. ¶ 95.

The Glupteba botnet's infiltration of infected computers and theft of information is precisely the activity the CFAA is designed to prevent. As the Second Circuit has observed, the Act was "enacted . . . to address 'computer crime,'" which was "principally understood as 'hacking' or trespassing into computer systems or data." *Valle*, 807 F.3d at 525; *see also Microsoft Corp. v. Does 1–18*, 2014 WL 1338677, at *6 (E.D. Va. Apr. 2, 2014) ("The CFAA was designed to prevent the sort of unauthorized access and other fraudulent activity effectuated by malware and

botnet activity"). Accordingly, courts have consistently upheld relief under the CFAA in circumstances similar to those presented here. *See, e.g.*, *Microsoft Corp. v. Does 1–2,* 2021 WL 4260665, at *3 (E.D.N.Y. Sept. 20, 2021) (granting default judgment to Microsoft where defendants allegedly used a botnet to infect Microsoft customers' computers and access their data); *Facebook, Inc. v. Fisher*, 2009 WL 5095269, at *1 (N.D. Cal. Dec. 21, 2009) (granting TRO where defendants allegedly engaged in a spamming and phishing scheme designed to steal Facebook login credentials); *Microsoft Corp. v. Does 1–51*, 2018 WL 3471083, at *1 (N.D. Ga. June 18, 2018) (granting TRO where defendants allegedly used a botnet to infect Microsoft customers' computers and steal sensitive information); *Physicians Interactive v. Lathian Sys., Inc*., 2003 WL 23018270, at *6 (E.D. Va. Dec. 5, 2003) (granting TRO where defendant allegedly used software to hack a website and file server to obtain proprietary information without authorization).

For all of these reasons, Google's CFAA claim not only raises substantial legal questions but is likely to succeed on the merits.

Electronic Communications Privacy Act ("ECPA"). Defendants also have violated the ECPA. The ECPA prohibits "intentionally access[ing] without authorization a facility through which an electronic communication service is provided" to "obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701(a). This provision is designed primarily to protect third-party entities that store information on behalf of users. *See In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001); *In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d 589, 609 (9th Cir. 2020), *cert. denied sub nom. Facebook, Inc. v. Davis*, 141 S. Ct. 1684 (2021) (Mem.) ("The text and legislative history . . . demonstrate that [it] was driven by congressional desire to protect third-

party entities that stored information on behalf of users"). Thus, accessing emails without authorization violates the ECPA. *Id.* (collecting cases).

Gmail and other Google platforms—a provider of email services—is a quintessential example of an electronic communications service provider. *See, e.g.*, *In re DoubleClick*, 154 F. Supp. at 512; *Kornotzki v. Jawad*, 2020 WL 2539073, at *3 (S.D.N.Y. May 19, 2020); *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 755–56 (N.D. Ohio 2013) (noting that a Gmail server is a "facility"). The botnet actors deliberately break into the accounts of Google users and obtain unauthorized access to emails and other communications stored on Google servers with the intent of acquiring user credentials. This is a clear violation of the statute. *See Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008) (accessing Gmail accounts without authorization violates the ECPA).

Lanham Act. Among the most popular of Google's services is YouTube, a widely used video-sharing service Google acquired in 2006. *See* Compl. ¶¶ 9, 162. The YouTube trademark is protected by incontestable federal registrations and embodies the valuable reputation and goodwill Google has earned in the marketplace over decades. *Id.* ¶ 165. Defendants' conduct in operating the Glupteba botnet undermines Google's valuable trademarks and violates the Act.

Section 1114 of the Act prohibits infringement of a trademark. This occurs when any person, without the consent of the trademark registrant, "use[s] in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services" and "such use is likely to cause confusion, or to cause mistake, or to deceive." 15 U.S.C. § 1114(1). To state a claim under this provision, a plaintiff need only allege that (1) it has a valid, protectable trademark and (2) that defendants' use of that trademark in commerce is likely to cause confusion among consumers.

Victorinox AG v. B & F Sys., Inc., 114 F. Supp. 3d 132, 139 (S.D.N.Y. 2015) (citing *Virgin Enters. Ltd. v. Nawab*, 335 F.3d 141, 146 (2d Cir. 2003)). Section 1125(a) similarly prohibits "false designations of origin" that are likely to cause confusion as to the "origin, sponsorship, or approval" of a product or service. 15 U.S.C. § 1125(a)(1)(A). A claim under that provision has the same elements as a claim under § 1114(1) and can be established with the same evidence. *Victorinox AG*, 114 F. Supp. 3d at 139.

Defendants' liability under these provisions is straightforward. Defendants seek to grow the botnet in part by using or engaging agents to use the YouTube mark to deceive users into downloading malware. Compl. ¶¶ 33, 102; Huntley Decl. ¶ 23. Defendants purport to offer YouTube video download programs—which, in reality, cause the user to download the Glupteba malware—and even go so far as to use the YouTube mark in domain names such as video-youtube-get.ru and on the website landing page. Compl. ¶¶ 33, 102; Huntley Decl. ¶ 23. This blatant exploitation of the well-known YouTube mark is likely to cause confusion among consumers and deceive the public. Indeed, that is the very point: By deceiving users into downloading the YouTube mark, Defendants perpetuate their criminal enterprise and garner significant profits.

Defendants' deceptive marketing also violates the Lanham Act's prohibition of false advertising. Section 1125(a)(1)(B) makes unlawful a false or misleading representation, including a false designation of origin, that "in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of . . . goods, services, or commercial activities." 15 U.S.C. § 1125(a)(1)(B). To establish liability under this provision, a plaintiff must show that (1) the advertising is "literally false" or "likely to deceive or confuse customers"; (2) the defendants "misrepresented an inherent quality or characteristic of the product"; (3) the defendant placed the statement in interstate commerce; and (4) "the plaintiff has been . . . injured as a result

of the misrepresentation," which may include "a lessening of goodwill associated with its products." *Merck Eprova AG v. Gnosis S.p.A.*, 760 F.3d 247, 255 (2d Cir. 2014) (cleaned up). Here, as discussed above, Defendants deceive internet users by falsely marketing their malware as software for downloading videos from YouTube, to the detriment of Google and Google's trademarks. That fraudulent marketing scheme establishes all of the elements of false advertising.

Courts have consistently granted relief under the Lanham Act where botnet operators exploit well-known trademarks to deceive consumers and gain unauthorized entry to their computers or accounts. *See, e.g.*, *Microsoft Corp. v. Does 1–2,* No. 1:20-cv-01217 (E.D.N.Y. Mar. 5, 2020), Dkt. 11 (granting TRO and holding that defendants' use of Microsoft trademarks to infiltrate the Windows operating system was designed to cause confusion, in violation of the Lanham Act); *Microsoft Corp. v. Does 1–18*, 2014 WL 1338677, at *8–9; *Microsoft Corp. v. Does 1–51*, 2018 WL 3471083, at *1 (holding that defendants had engaged in practices violating the Lanham Act). This Court should follow the same course here.

RICO. Google is also likely to prevail on its claims under RICO. To prove a RICO claim, a plaintiff must establish that the defendant engaged in "(1) conduct (2) of an enterprise (3) through a pattern (4) of racketeering activity." *DeFalco v. Bernas*, 244 F.3d 286, 306 (2d Cir. 2001) (cleaned up). As detailed in the Complaint, the Glupteba Enterprise is the modern incarnation of organized crime. Compl. ¶¶ 1–4, 109–115. Google can satisfy each of the required elements of a RICO claim for each Defendant.

First, to establish the conduct element, a plaintiff must establish that the defendant had "some part in directing [the enterprise's] affairs." *DeFalco*, 244 F.3d at 309 (cleaned up). This standard is "not limited to those with primary responsibility," nor is it limited to those "with a formal position in the enterprise." *Id.* Each Defendant has a significant role in the Enterprise,

indicating that each Defendant had at least "some part" in the Glupteba Enterprise. *See* Compl. ¶¶ 92–95; Huntley Decl. ¶¶ 87–89.

Second, to establish the enterprise element, a plaintiff must establish (1) "a common purpose of engaging in a course of conduct"; (2) "an ongoing organization, formal or informal"; and (3) "evidence that the various associates function as a continuing unit." *DeFalco*, 244 F.3d at 307. The common purpose of the Glupteba Enterprise is clear: spread malware to build a botnet that is then deployed for numerous criminal schemes, for profit. Defendants work together to accomplish this purpose, each playing a role described above. Furthermore, there are numerous connections among the individual Defendants, corporate Defendants, and the domains through which they effect their criminal schemes. All the individuals and entities involved in these schemes are connected to each other and to the Enterprise's criminal schemes. *See* Compl. ¶¶ 3, 89–95; Huntley Decl. ¶¶ 87–89. Google's investigation has shown that they are linked across various Gmail accounts, roles in domains used as part of the Enterprise, connected IP addresses, and even physical addresses. *See* Compl. ¶¶ 3, 89–95; Huntley Decl. ¶¶ 87–89. Google has thus marshaled strong evidence that Defendants are a group of persons associated together, as a continuing unit, for the common purpose of carrying out the criminal activities of the Enterprise.

Third, to establish the pattern element, a plaintiff must establish "at least two acts of racketeering activity, one of which occurred [after 1970] and the last of which occurred within ten years . . . after the commission of a prior act of racketeering activity." *DeFalco*, 244 F.3d at 306 (quoting 18 U.S.C. § 1961(5)). Google has presented numerous examples of the Enterprise's recent criminal conduct that clearly forms a "pattern" within the meaning of the statute. *Fourth*, to establish the racketeering activity element, a plaintiff must establish that the defendant committed one or more of the predicate acts enumerated in 18 U.S.C. § 1961(1). *See DeFalco*,

244 F.3d at 306. The predicate acts include violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, federal wire fraud statute, 18 U.S.C. § 1343, federal identity fraud statute, 18 U.S.C. § 1028, and federal access device fraud statute, 18 U.S.C. § 1029. As detailed above, Defendants violated the CFAA in multiple ways by infecting users' computers with malware "droppers" to infiltrate their systems, infecting them with malware modules to carry out criminal activities, and sending commands to the infected systems. *See supra* at 11–15.

Those CFAA violations are sufficient to satisfy the "predicate acts" element of a RICO claim. Yet Google has identified several other predicate acts as well. For example, the Glupteba Enterprise also committed wire fraud in multiple ways by "transmitt[ing], by means of wire . . . communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing [fraudulent] scheme[s]." 18 U.S.C. § 1343. *First*, each time that the Enterprise facilitates an unauthorized login to a Google user's account by a person other than the true Google user, the Enterprise deceives Google as to the true identity of the person accessing the Google user's account. Compl. ¶ 127. *Second*, the Enterprise defrauds users each time it tricks them into downloading the Glupteba malware, such as by exploiting the use of a fake website featuring the YouTube mark. *Id.* And *third*, the Enterprise deliberately markets credit cards to facilitate the fraudulent purchase of ads on Google or other Google services. *Id.* ¶ 129. In addition, Defendants have used their unauthorized access to victims' computers to steal personal information and thereby have committed identity fraud by "knowingly transfer[ring], possess[ing], [and] us[ing], without lawful authority, a means of identification of another person" in connection with "unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable State or local law." 18 U.S.C. § 1028. And Defendants have committed access device fraud by "knowingly and with intent to defraud traffic[king] in or us[ing] one or more

unauthorized access devices," in the form of stolen passwords, credentials, and other account information, "to obtain[] anything of value aggregating $1,000 or more" during a one-year period. *Id.* § 1029(a)(2). As described above, Defendants use Glupteba malware to steal this account information and then sell it on virtual storefronts such as Dont.farm, where cybercriminals exploit it for a variety of profitable schemes, such as commercialized ad fraud and phishing. For example, customers of the Enterprise pay for the ability to access a browser that is already logged into a victim's Google account. *See* Compl. ¶ 56. Google can thus show that Defendants committed at least two (in fact, many more) of the predicate acts required for RICO liability, all of which have injured Google's business or property. Compl. ¶¶ 116–136.

In addition to establishing a substantive RICO violation, Google can demonstrate that Defendants engaged in a RICO conspiracy. To establish that claim, Google need only prove that Defendants "conspire[d] to violate" the provisions of 18 U.S.C. § 1962(c). The overlapping links among the Defendants and between the Defendants and the Glupteba botnet's operations, including common ties to the C2 server, indicate that Defendants formed an agreement to undertake the acts described above as part of a common scheme and conspiracy. *See* Compl. ¶¶ 89–95. By agreeing to form the Glupteba Enterprise and agreeing that the Enterprise would commit the thousands of predicate acts of fraud and related activity Google has uncovered, the Enterprise is liable for conspiring to violate 18 U.S.C. § 1962(c). Google is therefore likely to succeed on its RICO and RICO conspiracy claims.

C. The Balance of Equities Favors a Temporary Restraining Order.

The equities also favor a temporary restraining order. The criminal enterprise defrauds consumers and injures Google. There is no countervailing weight. There is no legitimate reason why Defendants should be permitted to continue to disseminate malware and control infected computers. *See, e.g.*, *US Airways, Inc. v. US Airline Pilots Ass'n*, 813 F. Supp. 2d 710, 736

(W.D.N.C. 2011) (balance of hardships favors injunction where enjoined activity is illegal); *Suber v. VVP Servs.*, 2021 WL 1101235, at *8 (S.D.N.Y. Mar. 23, 2021) (balance of hardships supported court's grant of an ex parte asset freeze injunction where defendants did not "have any right to use the profits of a fraudulent enterprise . . . to continue supporting their unlawful activities or for personal uses"); *FTC v. Verity Int'l, Ltd.*, 2000 WL 1805688, at *1 (S.D.N.Y. Dec. 8, 2000) (balance of equities weighs in favor of a temporary restraining order where defendant's practices likely violate a federal statute).

D. The Public Interest Favors a Temporary Restraining Order.

Finally, an injunction would serve the public interest. In recent months, as many as 60,000 devices became infected with Glupteba malware in a single day. With each day that passes, Defendants infect new computers, steal more account information, and deceive unsuspecting victims. And the public interest is clearly served by enforcing statutes designed to protect the public, such as the CFAA, ECPA, and Lanham Act. *See, e.g.*, *BSN Med., Inc. v. Witkowski*, 2008 WL 11511454, at *4 (W.D.N.C. Nov. 21, 2008) ("In a trademark case, the public interest is most often a synonym for the right of the public not to be deceived or confused." (cleaned up)).

II. The Temporary Restraining Order Must be Ex Parte.

Rule 65 authorizes courts to enter a temporary restraining order ex parte when the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(l). Under this rule, an order may be issued without notice if (1) "an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result" before hearing from the adverse party and (2) "the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required." *Id.* A temporary restraining order "may be ordered on an ex parte basis under subdivision (b) if the applicant makes a strong showing of the reasons why notice is likely to defeat effective relief."

Fed. R. Civ. P. 65 Comm. Notes on Rules. As such, even where notice could have been given to the adverse party, ex parte orders are proper when notice "appears to serve only to render fruitless further prosecution of the action." *In re Vuitton et Fils S.A.*, 606 F.2d 1, 5 (2d Cir. 1979) (per curiam); *see also Granny Goose Foods, Inc. v. Bhd. of Teamsters & Auto Truck Drivers Loc. No. 70*, 415 U.S. 423, 439 (1974).

Google has already set forth facts demonstrating immediate and irreparable harm. Advance notice should not be required here because if Defendants were notified before this Court issues a temporary restraining order, they would move swiftly to create an alternate C2 structure to continue carrying out their criminal enterprise. *See* Declaration of Laura Harris ("Harris Decl.") ¶¶ 3–10. They would likely also direct the infected computers to communicate through that structure before the temporary restraining order can have any remedial effects. In circumstances such as these, when notice would render relief ineffective, an ex parte temporary restraining order is appropriate. *See In re Vuitton*, 606 F.2d at 5.

Defendants' botnet operation is sophisticated and allows them to move their malicious infrastructure quickly. *See* Compl. ¶¶ 47–50; Huntley Decl. ¶¶ 33–42, 97. The effectiveness of Google's request relief thus depends largely on its being implemented before Defendants know about it. Huntley Decl. ¶ 97; Harris Decl. ¶¶ 3–10. Courts in this district and throughout the country have had no trouble finding that defendants engaged in illicit Internet enterprises that deploy botnets in similar schemes are "likely to delete or to relocate the botnet command and control," "destr[oy] or conceal[] . . . other discoverable evidence of Defendants' misconduct," and "warn their associates engaged in such activities" if given "advance notice of th[e] action." *E.g.*, *Sophos Ltd. v. Does 1-2*, 2020 WL 4722425, at *2 (E.D. Va. May 1, 2020); *Microsoft Corp. v. Does 1-51*, 2017 WL 10087886, at *2 (N.D. Ga. Nov. 17, 2017); *FTC v. Pricewert LLC.*, 2010

WL 329913, at *3 (N.D. Cal. Jan. 20, 2010) (issuing ex parte TRO suspending Internet connectivity of a company enabling botnet activity because otherwise the "[d]efendant is likely to relocate the harmful and malicious code").

This is also true of the Glupteba Enterprise. *See* Huntley Decl. ¶¶ 35–42, 97. Defendants' technological sophistication and ability to move their malicious infrastructure quickly pose a significant risk, if not certainty, that the botnet infrastructure will evade disruption if Defendants are given advance notice of Google's requested relief.

To ensure that the ex parte relief is strictly limited to "serving [its] underlying purpose" and no more, *Granny Goose Foods*, 415 U.S. at 439, Google also will undertake extraordinary efforts to provide actual notice to Defendants of the temporary restraining order and preliminary injunction hearing, and effect service of the complaint, temporary restraining order, and other papers filed in this matter, immediately upon effectuation of the injunctive relief in the proposed order, and in no event fewer than five days before the preliminary injunction hearing.

III. The Court Should Authorize Google to Serve Process by Alternative Means.

Google also requests permission to serve Defendants, who reside in Russia, by alternative means under Federal Rule of Civil Procedure 4(f)(3). *See* Harris Decl. ¶¶ 11–23. Google has obtained mailing addresses, email addresses, and phone numbers associated with Defendants and requests that the Court authorize Google to serve Defendants through as many of the following methods as are available: (1) mail, (2) email, (3) text message, and (4) notice through ICANN. *Id.*

Under Rule 4(f)(3), courts may authorize service through a variety of methods, "including publication, ordinary mail, mail to the defendant's last known address, delivery to the defendant's attorney, telex, and most recently, email." *Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1016 (9th Cir. 2002). As courts in this district have explained, "[i]t is well-settled that service by email on foreign defendants meets this standard in an appropriate case." *Elsevier, Inc. v. Siew Yee*

Chew, 287 F. Supp. 3d 374, 379 (S.D.N.Y. 2018). Here, text messages and emails are likely to be the most accurate and viable means of notice and service for these cybercriminal Defendants. Other courts have authorized service by email in similar circumstances. *See, e.g.*, *Microsoft Corp. v. Does 1–18*, 2014 WL 1338677, at *3 (citing *Rio Props.*, 284 F.3d at 1018); *see also Rio Props.*, 284 F.3d at 1014–18 (service by email appropriate). In addition, "combin[ing]" multiple means of alternative service reinforces their permissibility and effectiveness. *Juicero, Inc. v. Itaste Co.*, 2017 WL 3996196, at *3 (N.D. Cal. June 5, 2017); *see also Marvici v. Roche Facilities Maint. LLC*, 2021 WL 5323748, at *4 (S.D.N.Y. Oct. 6, 2021) (approving of service by text message as "one piece of a multi-prong approach to service").

As further confirmation that Google's proposed methods of service are reasonably calculated to provide actual notice and appropriate in these circumstances, Google will send notice by ordinary mail to the extent an address is available. Accordingly, the Court should authorize Google's request for alternative service in accordance with the accompanying proposed order.

IV. The All Writs Act Authorizes the Court to Direct Cooperation by Third Parties, Including Domain Registrars and Web Hosting Providers.

The Glupteba Enterprise uses domains and web servers hosted by third parties to disseminate the Glupteba malware, control infected devices, and operate online storefronts. *See* Compl. ¶¶ 36, 54. Google's proposed order, if entered by the Court, would direct these third-party registrars, web infrastructure companies, and web hosting providers to take down or suspend the infrastructure used by the Glupteba Enterprise, thus disrupting the botnet.

The All Writs Act provides that courts "may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651. Under well-established precedent, this language empowers courts to issue orders to non-parties. The power conferred by the Act extends, in "appropriate circumstances," to "persons who,

though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice." *Makekau v. State*, 943 F.3d 1200, 1205 (9th Cir. 2019). Notably, such jurisdiction may "encompass even those who have not taken any affirmative action to hinder justice." *Sprint Spectrum L.P. v. Mills*, 283 F.3d 404, 414 (2d Cir. 2002) (cleaned up). This "grant of authority to enjoin and bind non-parties to an action," when "needed to preserve the court's ability to . . . enforce its decision," is "[a]n important feature of the All Writs Act." *In re Baldwin-United Corp. (Single Premium Deferred Annuities Ins. Litig.)*, 770 F.2d 328, 338 (2d Cir. 1985).

To determine whether the writ requested is "necessary or appropriate" within the meaning of the Act, courts must consider: (1) whether the writ "unreasonabl[y] burdens" the third party at issue; (2) whether the writ is "necessary" or "essential to the fulfillment of the purpose" of a court order; and (3) whether the third party is "so far removed from the underlying controversy that its assistance could not be permissibly compelled." *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 172–78 (1977); *see also United Spinal Ass'n v. Bd. of Elections in City of N.Y.*, 2017 WL 8683672, at *5 (S.D.N.Y. Oct. 11, 2017), *report and recommendation adopted*, 2018 WL 1582231 (S.D.N.Y. Mar. 27, 2018) (same).

The narrowly tailored relief requested by Google satisfies these requirements. *First*, requiring these companies to suspend or take down the relevant infrastructure imposes minimal burdens. In *New York Telephone*, the Supreme Court noted that the telephone company "regularly employs [pen register] devices without court order" for its own business purposes. 434 U.S. at 174. Here, likewise, domain registrars and web infrastructure companies routinely suspend or terminate domain services in the ordinary course of business. The same is true for the hosting companies that maintain the C2 servers. *Second*, the writ requested is necessary to effectuate the

proposed order, the purpose of which is to disrupt the operations of the Glupteba botnet and the criminal network that profits from its proliferation. Just as the surveillance authorized in *New York Telephone* could not have been accomplished without the participation of the telephone company, the reasonable cooperation of the third-party registrars is required to deny Defendants' continued use of the Glupteba infrastructure. *See In re U.S. of Am. for an Ord. Authorizing an In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980). And, *third*, the third parties used for this infrastructure are not "so far removed" from the underlying criminal activity that their assistance cannot reasonably be compelled. *See N.Y. Tel.*, 434 U.S. at 174. They control the very domains and servers that allow the Glupteba botnet to operate.

In keeping with these principles, district courts across the country have repeatedly invoked the All Writs Act to grant relief similar to the relief requested here. *E.g.*, *Microsoft Corp. v. Does 1–82*, 2013 WL 6119242, at *3 (W.D.N.C. Nov. 21, 2013) (noting that the defendants had "engaged in illegal activity using the Internet domains" and ordering that the specified domains be "immediately transferred to the ownership and control of Microsoft"); *Microsoft Corp. v. Does 1–18*, 2014 WL 1338677, at *12–13 (ordering registrars of domains associated with a botnet to "transfer the domains . . . to the control of Microsoft"); *Microsoft Corp. v. Does 1–51*, 2017 WL 10087886, at *4 (ordering registrars to "tak[e] reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to control the botnets"); *Microsoft Corp. v. Does 1–2*, 2021 WL 4260665, at *4 (ordering domain registrars to "take reasonable steps to . . . prevent the domains from being controlled by the Defendants"). To protect the public from the serious threat posed by Glupteba, it is well within this Court's authority to order the takedown of the domains and servers specified in Appendix A.

V. Google Is Entitled to an Order Restraining Defendants' Transfer of Assets.

This Court may order a prejudgment freeze of a defendant's assets where, as here, a plaintiff seeks an accounting of the defendant's profits from Lanham Act trademark infringement violations. *See Gucci Am., Inc. v. Weixing Li*, 768 F.3d 122, 133 (2014) (upholding order of prejudgment freeze of defendant's assets where plaintiff sought accounting of profits on Lanham Act claim). Absent a freeze order, an accounting of profits—which is an equitable remedy available under the Lanham Act, *see* 15 U.S.C. § 1117—may be rendered impossible, and Google may ultimately be unable to recover damages.

Rule 64 of further provides that "[a]t the commencement of and throughout an action, every remedy is available that, under the law of the state where the court is located, provides for seizing a person or property to secure satisfaction of the potential judgment." Fed. R. Civ. P. 64. This includes injunctive relief under the relevant state's pre-trial attachment statute. *See Ayyash v. Bank Al-Madina*, 233 F.R.D. 325, 327 (S.D.N.Y. 2005) (granting plaintiff's request for ex parte attachment of assets pending adjudication of plaintiff's civil RICO claim). Under N.Y. C.P.L.R. 6212(a) and 6201(1), attachment is appropriate where the plaintiff shows a probability of success on the merits, that the defendant is a non-domiciliary residing outside of the state, and the amount demanded exceeds known counterclaims. *See id.* Those elements are plainly met here.

CONCLUSION

Google respectfully requests that this Court grant its motion for a temporary restraining order, asset freeze order, and order to show cause why a preliminary injunction should not issue. Google further requests further that the Court permit notice of the preliminary injunction hearing and service of the complaint by alternative means.

DATED: December 2, 2021

Respectfully submitted,

Laura Harris
Andrew Michaelson
Kathleen E. McCarthy
Matthew Bush
KING & SPALDING LLP
1185 Avenue of the Americas, 34th Floor
New York, NY 10036
Telephone: (212) 790-5356
Fax: (212) 556-2222
lharris@kslaw.com
amichaelson@kslaw.com
kmccarthy@kslaw.com
mbush@kslaw.com

Sumon Dantiki (*pro hac vice* to be submitted)
David P. Mattern (*pro hac vice* to be submitted)
KING & SPALDING LLP
1700 Pennsylvania Ave., NW, 2nd Floor
Washington, DC 20006
Telephone: (202) 626-5591
Fax: (202) 626-3737
sdantiki@kslaw.com
dmattern@kslaw.com

Bethany L. Rupert (*pro hac vice* to be submitted)
KING & SPALDING LLP
1180 Peachtree Street, NE, Suite 1600
Atlanta, GA 30309
Telephone: (404) 572-3525
Fax: (404) 572-5100
brupert@kslaw.com

Counsel for Plaintiff Google LLC